Adabas Security

Adabas provides the following facilities to prevent unauthorized access to and/or updating of Adabas database files:

- Adabas data encryption (ciphering) which provides data security;
- Adabas multiclient files to control access to records in a file;
- Adabas Security and the related security utility ADASCR, a selectable unit, which provides selective user access/update protection at a file, field, and field value level; and
- Adabas SAF Security (ADASAF), a selectable unit, which provides control of Adabas resources at a database/utility, command, or file level through standard security packages based on the System Authorization Facility (SAF) such as RACF, CA-ACF2, and CA-Top Secret. ADASAF is initially available for OS/390, z/OS, and OS IV/F4 (FACOM) operating systems only.

Note:
It is planned that Adabas SAF Security will extend support to all supported operating system in a subsequent release of Adabas.

Security is accomplished by comparing passwords and authorization levels.

This chapter covers the following topics:

- Data Encryption
- Multiclient Files
- Adabas Security and ADASCR
- Adabas Interface to SAF-based Packages
- Related Security Options

Data Encryption

Data encryption is an integral feature of Adabas and requires no options or extra modules. Data may be enciphered before being placed in the database.

The user must provide the cipher key at the time records are stored. This key is not stored and must be available to request or decipher the data. This minimizes the chances of data being compromised by unauthorized access to the system.

To retain maximum control over cipher codes, an Adabas user exit program can be created to insert the currently valid cipher code into user applications; this removes the need to make the codes known to users, and protects the file from corruption that can occur by adding data that is encrypted with the wrong cipher code.

Multiclient Files

Also available as an integral feature of Adabas that requires no options or special modules is the multiclient file.

A single Adabas physical file defined as "multiclient" can store records for multiple users or groups of users. The multiclient feature divides the physical file into multiple logical files by attaching an internal owner ID to each record.

The owner ID is assigned to a user ID. A user ID can have only one owner ID, but an owner ID can belong to more than one user. Each user can access only the subset of records that is associated with the user’s owner ID.

Note:
For any installed external security package such as RACF or CA-Top Secret, a user is still identified by either Natural ETID or LOGON ID.

All database requests to multiclient files are handled by the Adabas nucleus.

Adabas Security and ADASCR

Access/update control is available only with Adabas Security and the related security utility ADASCR that defines and controls Adabas Security functions.

Adabas Security provides two levels of protection: access/update and value.

Access/Update Level Protection

"Access-/update-level"protection applies a basic level of security on a file-by-file basis. Access/update protection can be defined for some files and not for others. It restricts use of a file or field within the file to those having an appropriate access/update profile definition and a password specified by the user of the file.

Access/update permission values ranging from 0 to 14 are defined for each user and attached to that user’s password, and each protected file (and selected field or fields, if desired) has equivalent access/update "threshold" protection values of the same range. Only a user whose permission value equals or is greater than the protection level of the specified file (and, when applicable, field) is permitted to perform that operation type (access or update) on the file or field. An access/update permission level of 0 only allows access/update of unprotected files or fields with protection level 0 or no defined protection password.

Value Level Protection

"Value-level" protection applies restrictions on the type and range of values that can be accessed or updated in specific fields. The restrictions are applied according to user password (files with fields using value-level protection must be password-protected), can be for specific values or for value ranges, and can be either "accept" or "reject" criteria.

Adabas Interface to SAF-based Packages

The System Authorization Facility (SAF) is used by OS/390 and compatible sites to provide rigorous control of the resources available to a user or group of users. Compatible security packages such as IBM's RACF, Fujitsu's RACF executing under MSP, and Computer Associates' ACF2 or Top Secret allow the system administrator

- to maintain user identification credentials such as user ID and password; and
- to establish profiles determining the datasets, storage volumes, transactions, and reports available to a user.

Generally, a security package allows the system administrator to authorize a user's access to system resources. The security package then monitors all users and their resource usage to ensure that no unauthorized access or change occurs. Attempts by unauthorized users to use either the system or specific system resources are recorded and reported.

A user profile, which can be for a single user or a group of users, defines which system hardware and software resources a user is allowed to use. A resource profile defines access/update privileges for one or more devices, volumes, and/or programs (resources that must be used together to perform certain functions can be defined together in the same profile).

When a user logs on to the system, the security package uses the user's logon ID to identify that user's profile. Each time the user attempts to perform a task or access information, the security package uses information in its resource profiles to allow or deny access. Using the profile concept, the security package expands the single point of authorization-the logon ID-to provide extensive control over all system resources.

The resulting security repository and the infrastructure to administer it represent a significant investment. At the same time, the volume of critical information held by a business is constantly growing, as is the number of users referencing the data. The challenge of controlling these ever-increasing accesses requires a solution that is flexible, easy to implement and, above all, one that safeguards the company's investment.

Adabas SAF Security (ADASAF)

Adabas SAF Security (ADASAF) enhances the scope of SAF-based security packages by integrating Adabas resources into the central security repository. ADASAF enables

- a single control and audit system for all resources;
- industry-standard protection of Adabas data; and
- maximized return on investment in the security repository.

ADASAF operation can be tailored on a nucleus-by-nucleus basis, allowing great flexibility in its implementation. It comprises

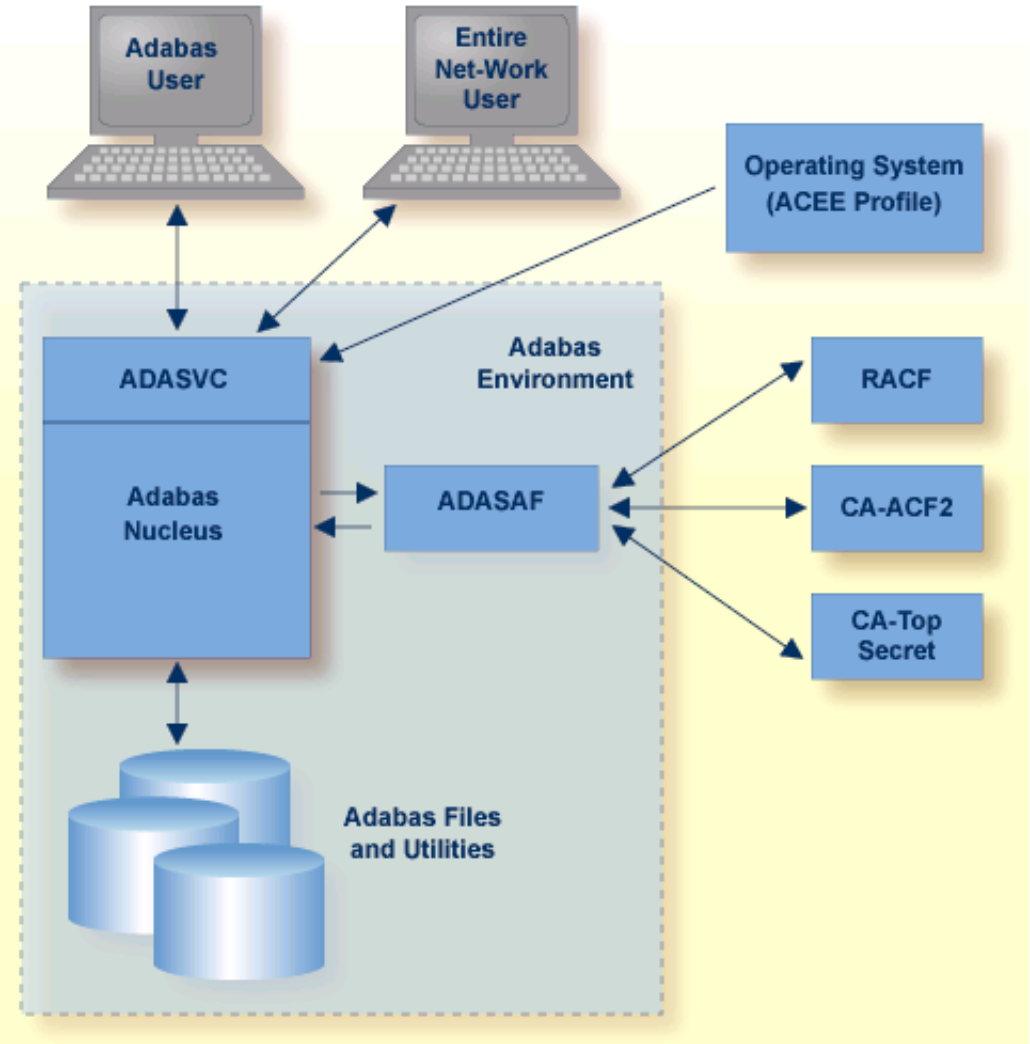
- a server operating in each secured Adabas address space;

- router extensions linked with the Adabas SVC;
- an online administration and monitoring system, an application written in Natural and accessed from either the demo or full version of Adabas Online System (AOS); and
- a plug-in routine PINSAF that interfaces with the Adabas error handling facility. It is activated automatically at initialization to aid problem diagnosis.

ADASAF allows you to protect the following Adabas resources:

Resource	Protection
Database Nucleus	Controls the users allowed to start an Adabas nucleus.
Adabas Utilities	Controls the users allowed to execute utilities by utility or database ID; for example, a user or group might be allowed to run ADAREP but not ADASAV against a particular database.
Database Files	Controls the users allowed to access database files.
Database Commands	Controls the users allowed to use access (READ/FIND) and update (STORE/UPDATE/DELETE) commands. To optimize performance, ADASAF disregards commands such as RC that are not file-specific.
Production Environment Data	Controls the users allowed to operate in a production or test environment. Such "cross-level" checking could be used, for example, to prevent damage by an application program inadvertently cataloged against the wrong database ID.
Transaction Data	Controls the users allowed to store or retrieve ET data.
Adabas Operator Commands	Controls the Adabas operator commands that can be issued from the system console.
File Passwords and Cipher Codes	Dynamically applies passwords and codes held in the security repository or supplied by a user exit. This eliminates the need for the application to manage security data and removes the requirement to transmit sensitive information from the client to the database.
Adabas Basic Services	Protects Adabas Basic Services at a selected level (main functions only or main functions and subfunctions) with defined resource profiles and controls user access to those profiles.

In the following figure, all traffic between database users and Adabas is controlled by the Adabas router. With ADASAF installed, the ADASAF router replaces the Adabas router and controls all access to Adabas:



The central security logon ID is used to log on to the system. Through the operating system or TP monitor, the installed external security package checks the authorization of the logon ID. For calls from a remote workstation or non-IBM platform, a remote logon procedure is used to give the logon ID to ADASAF. The router contains a security exit that extracts the user's logon ID from the ACEE for the user.

Full, flexible control is maintained with a *one user : one definition* approach while previous investments in host-based security systems and infrastructures are enhanced, not discarded.

Related Security Options

Adabas Online System Security

The demo version of Adabas Online System (AOS) distributed with Adabas includes a security facility for restricting access to the Adabas online facilities. AOS Security requires Natural Security as a prerequisite. See the *Adabas Security* documentation for more information.

Natural Security

The Natural Security system provides extensive security for Adabas/Natural users. It is required for AOS Security and recommended for other features of Adabas. See the *Natural Security* documentation for more information.

Using the SAF Repository to Secure Software AG Products

Adabas SAF Security or ADASAF is one of several Software AG security products that enhance the effectiveness of the SAF central security repository:

Product	Protects
Adabas SAF Security	Adabas
Adabas SQL Server SAF Security	Adabas SQL Server
Entire Net-Work SAF Security	Entire Net-Work version 5.6 and above
EntireX Security	EntireX, Entire Broker, Broker Services
Natural SAF Security	Natural

Entire Security SAF Gateway

Entire Security SAF Gateway can be installed under OS/390, MVS/ESA, MSP F4 EX and AE. Version 4.1.1 can be used to secure the following when using a SAF-compatible security system:

- Adabas (version 6.2 and earlier) for mainframes
- Adabas SQL Server operating in MVS environments
- Natural RPC using Entire Broker
- Natural for mainframes
- Entire Broker (pre-EntireX) operating in MVS, UNIX, and Windows environments (the security built into EntireX now protects Entire Broker and Broker Services as well).
- Entire Net-Work version 5.5 and lower (the Entire Net-Work SAF Security Interface is used for Entire Net-Work version 5.6 and above; see *Entire Net-Work SAF Security*).
- API Facility for Windows and UNIX applications

SAF Gateway protects client/server, peer-to-peer, and standard application systems. The software is implemented at specific points where communication between clients, servers, and peers is secured using definitions made in the SAF-based security system.

SAF Gateway comprises at least two separate components in any implementation:

- The main component, referred to as the SAF Gateway started task, operates in its own MVS address space as a gateway to SAF-based security systems. As a node in the Software AG network, it focuses SAF-based processing for the products being protected. The SAF Gateway started task can operate in combination with an existing Adabas database.

- The second component depends on what is being protected and represents the various different distributed and mainframe scenarios listed above. It can be located in the application software itself; for example, mainframe Natural. Distributed applications are protected by authenticating clients/servers and securing the communication between different components.

The API facility for Windows and UNIX applications is already being used to secure

- Web Servers operating under Windows NT and UNIX
- Visual Basic applications under Windows
- PowerBuilder applications under Windows
- Delphi applications under Windows
- C and C++ applications in Windows and UNIX

Entire Net-Work SAF Security (NETSAF)

The Entire Net-Work SAF Security (NETSAF) is a separate, optional product for OS/390 and z/OS environments running Entire Net-Work version 5.6 or above. It allows Entire Net-Work clients to access SAF-secured data sources (targets); for example, Adabas, Adabas SQL Server, Entire Broker, and Entire System Server.

NETSAF can be activated on a link-by-link basis. If only one node of several communicates externally, security can be activated for that node alone and only for external links.

To secure Entire Net-Work, it is necessary to define resource profiles in the SAF repository. Resource profiles are defined for each host target. Adabas resource profiles can be defined at the file level. The command type determines the access level required for successful authorization: valid access levels are READ, UPDATE, and CONTROL. CONTROL applies to AOS commands, for example.

Point-of-access verification of incoming requests is made against the SAF-based central security repository: all access from mainframe clients can be verified against the same security profile.

Security checks are based on a trusted user ID, which must exist in the central security repository. In some cases, the user ID is authenticated in the caller’s home environment or is fixed by, for example, the Entire Net-Work configuration. A user ID can be lost if calls are routed through an intermediate gateway node.